

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
ALEXANDER MIRVIS, BETTY BUTLER and LAINIE
FROEHLICH, individually and on behalf of others
similarly situated,

Plaintiffs,

-against-

BERKSHIRE HATHAWAY, INC. and GOVERNMENT
EMPLOYEES INSURANCE COMPANY (a/k/a GEICO),

Defendants.
-----X

Docket No. 21 Civ. 2210

**CLASS ACTION
COMPLAINT**

Jury Trial Demanded

Plaintiffs Alexander Mirvis, Betty Butler and Lainie Froehlich (“Plaintiffs”), individually and on behalf of all others similarly situated (the “Class” or “Class members”), bring this Class Action Complaint against Defendants Berkshire Hathaway, Inc. and Government Employees Insurance Company (a/k/a GEICO), based on their individual experiences and personal information, and investigation by their counsel.

INTRODUCTION

1. Plaintiffs, individually and on behalf of all others similarly situated, brings this class action suit against Defendants because of Defendants’ failure to safeguard the confidential information of millions of current and former GEICO customers. The confidential information stolen appears to be information contained on plaintiffs’ customers’ driver’s license numbers and others similarly situated.

2. Government Employees Insurance Company (hereinafter GEICO) is a nationwide automobile insurance company headquartered in Chevy Chase, Maryland and is a wholly owned subsidiary of Berkshire Hathaway, Inc. (hereinafter Berkshire), a conglomerate holding company headquartered in Omaha, Nebraska. With over fifteen million policy holders, GEICO collects a

significant amount of data from its current and former policy holders, often including sensitive personal information obtained in the context of an insurance relationship, such as Social Security numbers, addresses, telephone numbers, date of birth, bank account numbers, credit card numbers, financial transaction records, credit ratings and driver's license numbers.

3. On or about April 9, 2021, GEICO announced by letters entitled "Notice of Data Breach" to its policy holders that between November 24, 2020 and March 1, 2021, personal information illegally obtained from other sources had been used to obtain unauthorized access to policyholders' driver's license numbers through the online sales system on GEICO's website, and that said information could be used to fraudulently apply for unemployment benefits in such policyholders' names (the "Data Breach"). The information accessed appears to have been information on plaintiffs' driver's licenses.

4. The confidential information that was compromised in the Data Breach can be used to gain unlawful access to the users' other online accounts, home addresses, legal names and to carry out identity theft or commit other fraud, can be disseminated on the internet and be available to those who broker and traffic in stolen PII.

5. While the sophistication of the methods employed in effectuating the Data Breach is not publicly known, it is certain that the Data Breach could have been avoided through basic security measures, authentications, and training.

6. At all relevant times, Defendants promised and agreed in various documents to safeguard and protect Personal Identifiable Information (PII) in accordance with federal, state, and local laws, and industry standards, including the New York SHIELD Act. Defendants made these promises and agreements on their websites and other written notices and also extended this commitment to situations in which third parties handled PII on their behalf.

7. Contrary to these promises, and despite the fact that the threat of a data breach has been a well-known risk to Defendants, especially due to the valuable and sensitive nature of the data Defendants collect, store and maintain, Defendants failed to take reasonable steps to adequately protect the PII of GEICO's current and former policyholders. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII.

8. As a result of Defendants' failure to take reasonable steps to adequately protect the PII of current and former GEICO policyholders, Plaintiffs' and Class members' PII is now readily available on the internet for anyone and everyone to acquire, access, and use for unauthorized purposes for the foreseeable future.

9. Defendants' failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiffs and Class members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy.

10. Accordingly, Plaintiffs seeks to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because Plaintiffs and Defendants are citizens of different states. Subject matter

jurisdiction is also based upon the Federal Trade Commission Act (FTCA). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendants as they conduct substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in the Data Breach was likely stored and/or maintained in accordance with practices emanating from this District.

13. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District, and because Plaintiffs reside within this District.

THE PARTIES

14. Plaintiff Alexander Mirvis is an individual GEICO policyholder residing in the County of Kings, State of New York.

15. Plaintiff Betty Butler is an individual GEICO policyholder residing in the County of Queens, State of New York.

16. Plaintiff Lainie Froehlich is an individual GEICO policyholder residing in the County of Suffolk, State of New York.

17. Defendant GEICO is an insurance company, a wholly owned subsidiary of Defendant Berkshire, authorized to conduct business in the State of New York, which conducts business within the State of New York and within this District, with its headquarters located in Chevy Chase, Maryland.

18. Defendant Berkshire is a domestic business corporation, organized and existing by virtue of the laws of the State of New York, authorized to conduct business in the State of New

York, which conducts business within the State of New York and within this District, headquartered in Omaha, Nebraska.

FACTUAL ALLEGATIONS

19. At all pertinent times, Plaintiffs were policyholders of insurance written by GEICO. In the course of purchasing insurance, Plaintiffs were required to provide certain personal and financial information to GEICO, including name, address, Social Security number, vehicle information, and driver's license number.

20. On or about April 9, 2021, Defendant GEICO advised Plaintiffs by letter that personal information illegally obtained from other sources had been used to obtain unauthorized access to their driver's license numbers through the online sales system on GEICO's website, and that said information could be used to fraudulently apply for unemployment benefits in such policyholders' names (the "Data Breach"). The information accessed appears to have been the plaintiffs' driver's licenses, drivers' license number, legal names, addresses, etc. Each Plaintiff has already determined that false claims have already been filed under their names for illicit purpose including filing for unemployment benefits.

21. Plaintiffs and Class members were required to agree to GEICO's Privacy Policy, Terms of Use, Payment Authorization, and Consent to Electronic Transactions and Disclosures.

22. GEICO promised to protect the PII of its policyholders and emphasizes its purported commitment to protection of PII. GEICO's website claims:

Protecting your privacy is very important to us. Customers have trusted us with their insurance needs since 1936, and we take our obligation to safeguard and secure personal information very seriously. We want you to understand how we protect your privacy and when we collect, use, and share information.

We restrict access to your Information to employees who we have determined need it to provide products or services to you. We train

our employees to safeguard customer information, and we require them to sign confidentiality and non-disclosure agreements. We maintain a variety of physical, electronic, and procedural safeguards to protect your Information from unauthorized access by third parties.

Information about our former customers and about individuals who have obtained quotes from us is safeguarded to the same extent as Information about our current policyholders.

23. GEICO has failed to maintain the confidentiality of PII, failed to prevent cybercriminals from access and use of PII, failed to avoid accidental loss, disclosure, or unauthorized access to PII, failed to prevent the unauthorized disclosure of PII, and failed to provide security measures consistent with industry standards for the protection of PII, of its current and former policyholders.

24. The “Notice of Breach” dated April 9, 2021 does not state when the breach was discovered except that it was “recently determined.”

25. This data breach was foreseeable, in light of the much-publicized wave of data breaches in recent years. Since at least 2015, the Federal Bureau of Investigation (“FBI”) has specifically advised private industry about the threat of “Business E-Mail Compromise” (“BEC”). The FBI calls BEC “a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide.” The FBI notes that “scammers’ methods are extremely sophisticated,” and warns companies that “the criminals often employ malware to infiltrate company networks.”¹

26. Accordingly, both GEICO and Berkshire knew, given the vast amount of PII it collects, manages, and maintains, that they were targets of security threats, and therefore

¹ BUSINESS E-MAIL COMPROMISE: AN EMERGING GLOBAL THREAT, <https://www.fbi.gov/news/stories/business-e-mail-compromise> (last visited Apr. 20, 2020).

understood the risks posed by unsecure data security practices and systems. Defendants' failure to heed warnings and to otherwise maintain adequate security practices resulted in this Data Breach.

27. Defendants, at all relevant times, had a duty to Plaintiffs and Class members to properly secure their PII, encrypt and maintain such information using industry standard methods, train their employees, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class members, and promptly notify Plaintiffs and Class members when Defendants became aware of the potential that its current and former policyholders' PII may have been compromised.

28. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and the Class members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted Defendants with their PII as part of receiving insurance coverage from GEICO. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiff and Class members.

29. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities such as Defendants.

30. Defendants' duty to use reasonable security measures also arose under New York's SHIELD Act (General Business Law § 899-bb), requiring businesses that collect private information on New York residents to implement reasonable cybersecurity safeguards to protect

that information. It mandates the implementation of a data security program, including measures such as risk assessments, workforce training and incident response planning and testing, and became effective on or about March 21, 2020. It covers all employers, individuals or organizations, regardless of location, that collect private information on New York residents. Its definition of PII includes driver's license numbers.

31. The Federal Trade Commission has established data security principles and practices for businesses as set forth in its publication, *Protecting Personal Information: A Guide for Business*.² Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems. The FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system, and have a response plan ready in the event of a data breach. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." (17 C.F.R. § 248.201 (2013)).

32. The FTC has prosecuted a number of enforcement actions against companies for

² https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Apr. 18, 2020).

failing to take measures to adequately and reasonably protect consumer data. The FTC has viewed and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.

33. Defendants failed to maintain reasonable data security procedures and practices.

34. Accordingly, Defendants did not comply with state and federal law requirements and industry standards, as discussed above.

35. Defendants were at all times fully aware of their obligations to protect the PII of current and former policyholders. Defendants were also aware of the significant consequences that would result from its failure to do so.

36. To date, Defendants have merely offered identity theft and credit monitoring services at no charge for 12 months. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs’ and Class Members’ PII.

37. Furthermore, Defendants’ credit monitoring offer to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than upon the Defendants, to investigate and protect themselves from Defendants’ tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiffs and Class members in credit monitoring services upon discovery of the breach, Defendants merely sent instructions offering the services to potentially affected policyholders with the recommendation that they sign up for the services.

38. As a result of the data breach and Defendants’ failure to provide timely notice to Plaintiffs and Class members, Plaintiffs’ and Class members’ PII are now in the hands of unknown hackers, and Plaintiffs and Class members now face an imminent, heightened, and substantial risk

of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendants' conduct. Accordingly, Plaintiffs and the Class members have suffered "injury-in-fact." See *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

39. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiffs and Class members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PII, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and to deal with governmental agencies, including the New York State Department of Labor and all those administering unemployment benefits, as a result of fraudulent claims ostensibly made on their behalf.

CLASS ACTION ALLEGATIONS

40. Plaintiffs bring this action and seek to certify and maintain it as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on behalf of themselves, and the following proposed Classes (collectively, the "Class").

41. The Nationwide Class is defined as follows: All individuals residing in the United States whose PII was compromised in the data breach initially disclosed by GEICO on or about April 9, 2020.

42. The New York Class is defined as follows: All individuals residing in New York whose PII was compromised in the data breach initially disclosed by GEICO on or about April 9, 2020.

43. Excluded from each of the above proposed Classes are: Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their

immediate family members.

44. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery.

45. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

46. Numerosity. Fed. R. Civ. P. 23(a)(1). Pursuant to Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class includes potentially millions of individuals whose PII was compromised in the Data Breach. Class members may be identified through objective means, including by and through Defendants' business records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

47. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). Pursuant to Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

- (a) Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class members' personal and financial information, including by vendors;
- (b) Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs and Class members' PII;

- (c) Whether Defendants' conduct, practices, actions, and omissions, resulted in or were the proximate cause of the data breach, resulting in the loss of PII of Plaintiffs and Class members;
- (d) Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and Class members;
- (e) Whether Defendants breached their duty to provide timely and accurate notice of the data breach to Plaintiffs and Class members;
- (f) Whether and when Defendants knew or should have known that their computer systems were vulnerable to attack;
- (g) Whether Defendants failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiffs' and Class members' PII, including by vendors;
- (h) Whether Defendants breached express or implied contracts with Plaintiffs and the Class in failing to have adequate data security measures despite promising to do so;
- (i) Whether Defendants' conduct was negligent;
- (j) Whether Defendants' conduct was *per se* negligent;
- (k) Whether Defendants' practices, actions, and omissions constitute unfair or deceptive business practices;
- (l) Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their personal and financial information; and
- (m) Whether Plaintiffs and Class members are entitled to relief, including

damages and equitable relief.

48. Typicality. Fed. R. Civ. P. 23(a)(3). Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs, like all members of the Class, were injured through Defendants' uniform misconduct described above and asserts similar claims for relief. The same events and conduct that give rise to Plaintiffs' claims also give rise to the claims of every other Class member because Plaintiffs and each Class member are persons that have suffered harm as a direct result of the same conduct engaged in by Defendants and resulting in the data breach.

49. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4). Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs' attorneys are highly experienced in the prosecution of consumer class actions and data breach cases.

50. Superiority (Fed. R. Civ. P. 23(b)(3). Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual members of the Class because the amount of monetary relief available to individual Plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield Inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

51. Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)). In the alternative, this action may properly be maintained as a class action, because:

- (a) The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants; or
- (b) The prosecution of separate actions by individual members of the Class would create a risk of adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of other members of the Class not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or
- (c) Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

52. Issue Certification (Fed. R. Civ. P. 23(c)(4)). In the alternative, the common questions of fact and law, set forth above, are appropriate for issue certification on behalf of the proposed Class.

FIRST CAUSE OF ACTION FOR NEGLIGENCE
(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

53. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs “1” to “52” above as if set forth in full herein.

54. Defendants required Plaintiffs and Class members to submit non-public, sensitive PII for purposes of obtaining insurance through GEICO.

55. Defendants had, and continue to have, a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII. Defendants also had, and continue to have, a duty to use ordinary care in activities from which harm might be reasonably

anticipated, such as in the storage and protection of PII within their possession, custody and control and that of its vendors.

56. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between GEICO and its policyholders. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiffs and the Class members from a data breach.

57. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, including Plaintiffs' and Class members' PII, and including driver's license numbers. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII.

58. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII within their possession, custody and control.

59. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class members by failing to design,

adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII.

60. But for Defendants' negligent breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been released, disclosed, and disseminated without their authorization.

61. Plaintiffs' and Class members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' PII.

62. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiffs and Class members have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

63. Defendants' above-described wrongful actions, inaction, omissions, and want of

ordinary care that directly and proximately caused this data breach constitute negligence.

SECOND CAUSE OF ACTION FOR NEGLIGENCE *PER SE*
(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

64. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs “1” to “63” above as if set forth in full herein.

65. Pursuant to the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiffs and Class members.

66. The FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect the PII of Plaintiffs and Class members. The pertinent FTC publications and orders form part of the basis of Defendants’ duty in this regard.

67. Defendants required, gathered, and stored personal and financial information of Plaintiffs and Class members for insurance purposes.

68. Defendants violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiffs and Class members and not complying with applicable industry standards, as described herein.

69. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

70. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class members.

71. As a direct and proximate result of Defendants’ negligence *per se*, Plaintiffs and

Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

72. Defendants' violation of the FTCA constitutes negligence *per se*.

73. For the same reasons and upon the same bases, Defendants' violation of the New York SHIELD Act and New York GBL §349 constitutes negligence *per se*.

THIRD CAUSE OF ACTION FOR BREACH OF CONTRACT
(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

74. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs "1" to "73" above as if set forth in full herein.

75. Plaintiffs and Class members, upon information and belief, entered into express contracts with GEICO that included GEICO's promise to protect nonpublic PII provided to GEICO from disclosure.

76. There was offer, acceptance and consideration, the consideration being the premiums paid by Plaintiffs and Class members in exchange for insurance coverage pursuant to the terms of said agreements, including the provisions of those agreements pertaining to the protection of PII.

77. Plaintiffs and Class members have performed and satisfied all of their obligations

to GEICO, pursuant to their insurance agreements, except for those obligations they were prevented or excused from performing or satisfying.

78. Defendants breached their contractual obligations to protect the nonpublic PII they possessed and with which they were entrusted with when the information was accessed by unauthorized persons as part of the data breach.

79. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

80. The above constitutes breach of contract by Defendants.

FOURTH CAUSE OF ACTION FOR BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

81. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs "1" to "80" above as if set forth in full herein.

82. Defendants required Plaintiffs and Class members to provide PII, including their driver's license, driver's license numbers, legal name and address, as a condition of issuing insurance. In so doing, Plaintiffs and Class members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such

information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised, or stolen.

83. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

84. Defendants breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect their PII, including driver's license numbers, and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

85. As a direct and proximate result of Defendants' breach of implied contract, Plaintiffs and Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

86. The above constitutes breach of implied contract by Defendants.

FIFTH CAUSE OF ACTION FOR MISREPRESENTATION
(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

87. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs "1" to "86" above as if set forth in full herein.

88. A special, privity-like relationship existed between Defendants and Plaintiffs and Class members herein by virtue of their relationship as insurer and insured, imposing a duty upon Defendants to impart correct information to Plaintiffs and Class members.

89. The Defendants incorrectly represented to Plaintiffs and Class members that they would take appropriate measures to safeguard their PII and promptly notify them of a data breach.

90. Plaintiffs and Class members reasonably relied upon said representations in that they held Defendants in a position of trust as insurers.

91. As a direct and proximate result of Defendants' misrepresentation, Plaintiffs and Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

92. The above constitutes misrepresentation on the part of Defendants.

SIXTH CAUSE OF ACTION FOR BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

93. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs "1" to "92" above as if set forth in full herein.

94. A fiduciary relationship existed between Plaintiffs and Class members Defendants, in that Defendants were in a position of trust with respect to Plaintiffs and Class members as

insurers and recipients of Plaintiffs' and Class members' PII, and owed a duty to insure that the PII entrusted to them was safeguarded pursuant to common law and statute.

95. The Defendants engaged in misconduct, consisting of the failure to safeguard the PII of Plaintiffs and Class members that had been entrusted to them, in violation of the duty to exercise due care, their contractual obligations and their statutory obligations pursuant to the Federal Trade Commission Act ("FTCA"), the New York SHIELD Act, New York GBL §349(a) and other statutes.

96. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiffs and Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

97. The above constitutes breach of fiduciary duty on the part of Defendants.

**SEVENTH CAUSE OF ACTION FOR VIOLATION OF NEW YORK GENERAL
BUSINESS LAW §349**

(On behalf of Plaintiffs, the Nationwide Class and the New York Class)

98. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in paragraphs "1" to "97" above as if set forth in full herein.

99. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the

conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- (a) Defendants misrepresented material facts to Plaintiffs and Class members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- (b) Defendants misrepresented material facts to Plaintiffs and Class members by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiffs' and Class members' PII;
- (c) Defendants omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Plaintiffs' and Class members' PII;
- (d) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiffs' and Class members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);
- (e) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law §§ 899-aa(2) and 899-bb (SHIELD Act).

100. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class members) regarding the security of its network and aggregation of PII.

101. The misrepresentations upon which consumers (including Plaintiffs and Class members) relied were material misrepresentations (*e.g.*, as to Defendants' adequate protection of PII), and consumers (including Plaintiffs and Class members) relied on those representations to their detriment.

102. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiffs and other Class members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

103. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class members damages.

104. As a direct and proximate result of Defendants' violation of NY GBL §349, Plaintiffs and Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and

credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

105. The above constitutes violation of NY GBL §349.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the members of the Classes defined above, respectfully request that this Court:

- A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiffs as the Class representatives, and appoint the undersigned as Class counsel;
- B. Order appropriate relief to Plaintiffs and the Classes;
- C. Awarding Plaintiffs and the Class members actual, compensatory, and consequential damages;
- D. Awarding Plaintiffs and the Class members statutory damages and penalties, as allowed by law;
- E. Awarding Plaintiffs and the Class members restitution and disgorgement;
- F. Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the other class members;
- G. Awarding Plaintiffs and the Class members punitive damages;
- H. Enter injunctive and declaratory relief as appropriate under the applicable law;
- I. Award Plaintiffs and the Classes pre-judgment and/or post-judgment interest as prescribed by law;
- J. Award reasonable attorneys' fees and costs as permitted by law; and

K. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

Dated: Brooklyn, New York
April 21, 2021

Respectfully submitted,

HELD & HINES, L.L.P.
Attorneys for Plaintiffs and the Class

/s/ Philip M. Hines
2004 Ralph Avenue
Brooklyn, New York 11234
(718) 531-9700
phines@heldhines.com